A METHOD AND APPARATUS FOR PROCESSING CONFIDENTIAL CODES

The invention relates to the field of code-using apparatuses and of methods for processing codes. More precisely, the invention relates to the field of systems having confidential access codes, in particular of apparatuses and methods enabling access to certain operations to be made secure, such as transactions, and in particular monetary transactions.

Numerous security functions make use of a confidential code. This code is numerical and typically 2 to 12 digits long, and it is associated with an identity profile of the holder authorized to hold the code, enabling the holder to make use of certain protected functions, and it is only knowledge of the code that enables those functions to be unlocked.

Generalizing this means of authentication, in particular combining a code and a microprocessor card, has led to the development of attacks during which the holder of the code, under threat, is made to reveal the code.

Solutions have been sought in an attempt to avoid such attacks. Thus, the document "Alert pin for personal banking terminals" (IBM Disclosure Bulletin, Vol. 36, No. 5, pp. 309-312) describes a method and apparatus for processing confidential codes that uses an emergency code to enable an alert to be given of fraudulent use without warning the attacker.

An object of the invention is to simplify that type of apparatus and method, while minimizing the risks run by the holder of a code when subjected to such an attack, and while maintaining protection of the functions that are to be protected.

The invention thus proposes a method of processing confidential codes in a system having secure functions, the method comprising the steps consisting in:

- receiving a code;

- verifying a first entitlement for accessing a first function, and as determined by a first code;
- authorizing access to the first function if the first entitlement is recognized; and
- if the first entitlement is not recognized, using the code to verify a second entitlement as determined by a second code that is different from the first code, to trigger at least one second function without revealing the fact that the code does not make it possible to obtain the first entitlement;

the method being characterized in that the step of verifying the second entitlement comprises the operations consisting in: obtaining a new code from the first code by means of a second transformation that is the inverse of a first simple transformation that enables the holder of the first code to obtain the second code from the first code; and testing the new code by performing again the step of verifying the first entitlement.

By means of the invention, the victim can reveal a second code to the attacker: by means of the method of the invention, this second code is different from a first code which gives entitlement to access a first function; there is thus no access to the first function which remains protected; however the second code can give entitlement to trigger a second function that can act as a decoy to divert the aggressor away from attempting to access the first function. The aggressor who has been diverted away will not seek to apply further stress to the victim, so the risks run by the victim are consequently reduced. Nevertheless, this method remains simple to implement since the step of verifying the first entitlement is common both to the test which is applied to the code as entered directly into the system having secure functions, and to the test which is applied to the code as obtained after the second transformation.

Advantageously, the first function of the method of the invention is a bank transaction.

Advantageously, the steps of the method of the invention consisting in verifying the first and second entitlements, make use of a microprocessor card.

Advantageously, said first simple transformation of the method of the invention is performed by a unit shift of one character of the first code.

Advantageously, the method of the invention further comprises a disabling step if the step which consists in verifying whether the first entitlement has been performed more than a determined number of times without success.

Advantageously, the second function of the method of the invention consists in displaying a message selected randomly from a plurality of messages stating that access to the first function is not possible, but without specifying that the code is not the right code for obtaining the first entitlement.

Advantageously, the second simple transformation of the method of the invention is itself a function of parameters that are accessible on the microprocessor card.

In another aspect, the invention provides apparatus for controlling access to secure functions by means of a confidential code.

Advantageously, the apparatus comprises:

- means for receiving a code;
- means for using said code to verify a first entitlement for accessing a first function, and as determined by a first code;
- means for authorizing access to the first function if the entitlement is recognized; and
- if the first function is refused, means for using the code to verify a second entitlement as determined by a second code which is different from the first code in order to trigger at least one second function without revealing the fact that the code does not enable the first entitlement to be obtained;

and it is characterized in that the means for verifying the second entitlement perform operations consisting in obtaining a new code from the first code by means of a second transformation that is the inverse of a first simple transformation that enables the holder of the first code to obtain the second code from the first code, and executing again the step of verifying the first entitlement in order to test the new code.

Advantageously, the apparatus of the invention is a bank card terminal.

Advantageously, the apparatus of the invention is used to make a bank transaction secure.

Advantageously, the steps which consist in verifying the first and second entitlements make use of a digitally-recorded user profile.

Advantageously, the means of the apparatus of the invention for verifying the first and second entitlements make use of a microprocessor card.

Advantageously, said simple transformation of the apparatus of the invention is performed by a unit shift of one character of the first code.

Advantageously, the apparatus of the invention further comprises disabling means that are implemented if the first entitlement has been tested more than a determined number of times without success.

Advantageously, the second function of the apparatus of the invention is performed by means which display a message selected randomly from a plurality of messages stating that access to the first function is not possible, but without specifying that the code is not the right code for obtaining the first entitlement.

Advantageously, the second simple transformation of the apparatus of the invention is a function of parameters accessible on the microprocessor card.

The invention will be better understood on reading the following detailed description and from the accompanying drawings, in which:

- Figure 1 is a block diagram of the main unit making up a particular apparatus for implementing the invention; and

- Figure 2 is a flow chart summarizing the steps in an implementation of the method of the invention.

In a preferred but non-limiting embodiment of the apparatus of the invention, the apparatus is an automatic teller machine (ATM). As shown in Figure 1, it comprises in conventional manner a central processor unit (CPU) 1 which processes and exchanges information with a reader 2 for reading bank cards 10, and a keypad 3 (or any other interactive input device), to control a cash dispenser mechanism 4 and the bank card reader 2, and to cause messages to be displayed on a screen 5. The processing of information and the control of the mechanisms constituting the apparatus of the invention by means of the CPU 1 is based on interchanges with a memory unit 6.

A card 10 has its own microprocessor. This microprocessor corresponds to a profile of the holder authorized to hold a first code.

The holder also holds a second code which is used as an emergency code in the manner described below.

The user thus holds two codes. The first code is the user's usual confidential code giving entitlement to access a first function, and specifically in the example described herein, a monetary transaction of the ATM type.

The second code is an emergency code. A user under threat from an attacker can thus reveal this second code instead of revealing the confidential code.

This second code is easy to remember and it is obtained from the first code by a simple arithmetic transformation.

Preferably, the second code differs from the first code in one digit only, which digit is advantageously modified by only plus one or minus one relative to the digit in the same position in the first and second codes.

Also preferably, the apparatus of the invention is implemented using the following method which is descried with reference to Figure 2.

When a user wishes to obtain a first function 180, specifically cash to be dispensed from the apparatus of the invention, the user inserts the card 10 into the reader 2 and enters a code on the keypad 3.

The CPU 1 then starts a test procedure at 100, which procedure has the following successive steps.

The next step 105 is reading the user profile and clearing a count of the number of times the code has been entered.

A flag 110 is generated to indicate that the code has not yet been transformed.

There follows a step 115 in which the code is input.

The code is tested in a code testing step 120 to verify a first entitlement.

If the test 120 gives a negative result, then the code supplied to the apparatus of the invention does not correspond to the first code held by the user, i.e. does not correspond to the confidential code. The flag is tested at 130. If the flag shows that the code has not yet been transformed, the CPU 1 undertakes a test for a second entitlement and proceeds at 140 to derive a second transformation, which is the inverse of a first simple transformation enabling the holder of a first code to obtain a second code (an emergency code) on the basis of the first code.

A flag 145 is generated to show that the transformation 140 has been derived.

The code obtained by the derived transformation 140 is used to reproduce the step of verifying the first entitlement, with the code tester 120. If after transformation 140 the resulting code still does not correspond to the first code (the usual confidential code), then the code input at the start 100 is not the second code (the emergency code). For example, it might be a keying mistake by the user. The procedure continues by restarting the first flag test 130. However, this time, the flag test 130 detects that the second entitlement has already been tested (T=1). The procedure thus continues with wrong code processing 150 similar to that known to the person skilled in the art. More particularly, a test is made 190 on the number of times the code has been input. If this number reaches 3, for example, a disabling step 200 is performed to end the procedure at 210. If the number is less than 3, then the user is asked at 220 if the procedure is to be abandoned. If so, the procedure ends at 210, otherwise the code must be input again after the flag 110 has been reinitialized.

If the code test 120 gives a positive result, then a second flag test 160 is performed. If the flag shows that the code has not been transformed, then the user has access to the protected function 180 (e.g. cash is dispensed). If the flag shows that the code has already been transformed, then the code which has successfully passed the first entitlement test is a code that had previously been subjected to the derived transformation operation 140. The code input at the start 100 of the procedure was therefore the emergency code. The procedure then continues with a second function 170, and specifically an emergency transaction 170 which can be a decoy function.

In the presently described example, the second function 170 corresponds to an emergency transaction which can cover various solutions.

One solution can consist in causing a message to be displayed on the screen 3, which message is selected randomly from a plurality of messages stating that access to the first function 180 is not possible, but without revealing that the code supplied to the apparatus of the invention is not the right code for obtaining the first entitlement.

For example, the message could be of the type "transaction temporarily unavailable" or "insufficient credit" or indeed any other one of the messages commonly used to inform a user of a fault in an ATM or of a problem in the holder's account.

In another solution, the normal cash dispensing procedure is initiated, e.g. by requesting the amount desired, and then whether the user requires a receipt, but a breakdown is then simulated and the requested amount is not dispensed.

In another solution, a sum is indeed dispensed, but only some limited amount, e.g. the minimum that can be dispensed.

The second simple transformation 140 makes it possible to discover the first code (the usual confidential code) on the basis of the second code (the emergency code). Advantageously, this second simple transformation 140 is variable, e.g. as a function of parameters accessible on the microprocessor card. For example, for a particular banking organization, the second transformation 140 can consist in incrementing the second digit of the code by one, whereas for some other organization, the transformation can consist in decrementing the last digit by one. The second transformation 140, and in particular which way a digit is to be varied, can also depend on whether or not the number constituting the "bank code", the "branch code", etc. is odd or even.

Numerous other possibilities can be envisaged.

Another advantage of the invention in the form described above is that only one code needs to be tested by the microprocessor of the card 10. Cards 10 presently in use are therefore compatible with this embodiment of the invention and there is no need to change cards 10 already in circulation.

It will nevertheless be understood that it is possible to use cards 10 that enable mutually independent first and second codes to be tested without performing the second transformation 140, and without going beyond the spirit of the invention.

It will also be understood that the above detailed description relates to ATM type apparatuses, but that the invention is equally applicable to terminals for payment by bank card and to any type of system having a secure function 180, for example certain computer systems, certain military or industrial sites, etc.

Instead of testing the code input in combination with the microprocessor card 10 in order to gain access to systems having a secure function 180, it is possible to envisage testing it in combination with the name of a user, or with any other part of a user profile.

The second function 170 described above is a decoy function simulating a misfunction of the system to be protected. In some cases, it could be envisaged that the second function 170 causes an alarm signal to be triggered, a defensive gas to be emitted, etc.